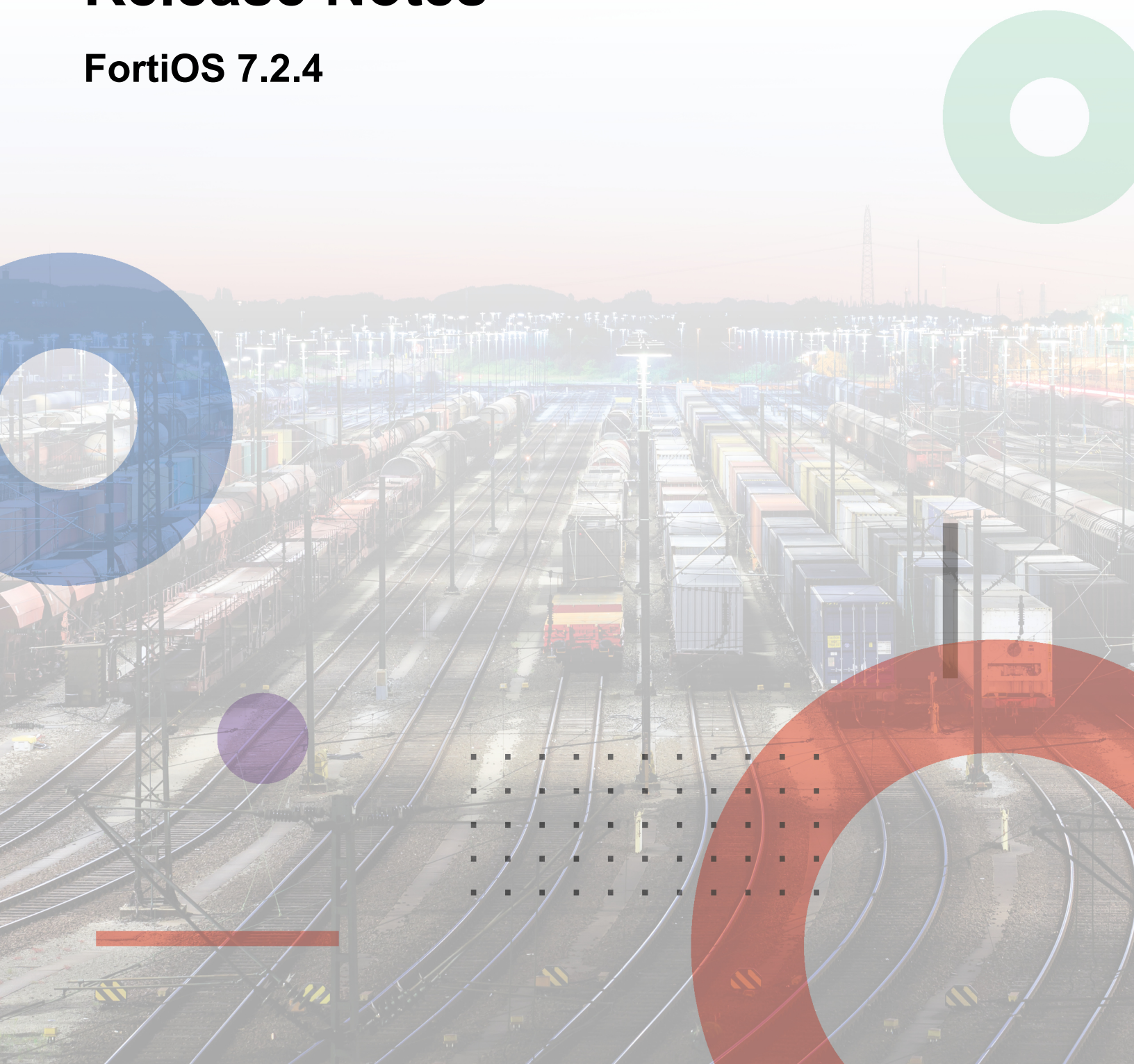
FORTINET

# Release Notes

## FortiOS 7.2.4



**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

January 31, 2023
FortiOS 7.2.4 Release Notes
01-724-846881-20230131

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2023-01-31 | Initial release. |

# Introduction and supported models

This guide provides release information for FortiOS 7.2.4 build 1396.

For FortiOS documentation, see the Fortinet Document Library.

## Supported models

FortiOS 7.2.4 supports the following models.

| | |
|---|---|
| **FortiGate** | FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1 |
| **FortiWiFi** | FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE |
| **FortiGate Rugged** | FGR-60F, FGR-60F-3G4G |
| **FortiFirewall** | FFW-3980E, FFW-VM64, FFW-VM64-KVM |
| **FortiGate VM** | FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN |
| **Pay-as-you-go images** | FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN |

# Special notices



## IPsec phase 1 interface type cannot be changed after it is configured

The IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

## Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.2.4 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features.

For more information, refer to the Hyperscale Firewall Release Notes.

# Changes in CLI

| Bug ID | Description |
|---|---|
| 729063 | Change ZTNA `firewall vip6` option from `arp-reply` to `ndp-reply`.<br>`config firewall vip6`<br>`edit "test"`<br>`set mappedip <IPv6_address>`<br>`set ndp-reply {enable \| disable}`<br>`next`<br>`end` |
| 751715 | Add command that allows users to switch between high-speed modem (USB 2.0, option `0`) and super-speed modem (USB 3.0, option `1`) operation mode.<br>`# execute lte-modem set-usb-mode {0 \| 1}` |
| 775793 | Add `shaping-stats` option under `config system npu` to enable/disable NP7 traffic shaping statistics.<br>`config system npu`<br>`set shaping-stats {enable \| disable}`<br>`end` |
| 785866 | Add command to collect FortiLink-related data in the FortiGate debug report.<br>`# diagnose debug fortilink-report {all \| switch-id \| switch-group}` |
| 796366 | Add `syslog-affinity` option to set the CPU mask for syslogd and its child process.<br>`config system global`<br>`set syslog-affinity <string>`<br>`end` |
| 797620 | Add `cert-probe-failure` option to allow/block the SSL-SSH profile deep inspection based on the certificate probe failure.<br>`config firewall ssl-ssh-profile`<br>`edit <name>`<br>`config ssl`<br>`set inspect-all deep-inspection`<br>`set cert-probe-failure {allow \| block}`<br>`end`<br>`next`<br>`end` |
| 815333 | Add option for the unknown ESP packets detection feature (default = `enable`).<br>`config system settings`<br>`set detect-unknown-esp {enable \| disable}`<br>`end` |

| Bug ID | Description |
|---|---|
| 818061 | Add diagnostic command to show the statistics of the SD-WAN peer' remote health checks.<br>`# diagnose system sdwan health-check remote <name> <seq_num>` |
| 823811 | Add `srcaddr6`/`dstaddr6` negate option in security policy configuration.<br>`config firewall security-policy`<br>`set dstaddr6-negate {enable \| disable}`<br>`set srcaddr6-negate {enable \| disable}`<br>`end` |
| 825479 | Add `restart` option in the `execute federated upgrade command`, which adds the ability to fail the multi-version upgrade in the event of a syntax error during the upgrade, and allows users to restart the currently configured upgrade through the CLI. |
| 826036 | Move `unknown-content-encoding` option from `antivirus profile` to `firewall profile-protocol-options`.<br>`config firewall profile-protocol-options`<br>`edit <name>`<br>`config http`<br>`set unknown-content-encoding {block \| inspect \| bypass}`<br>`end`<br>`next`<br>`end` |
| 836650 | Add `interface-subnet-usage` option under config system global to enable/disable interface subnet usage.<br>`config system global`<br>`set interface-subnet-usage {disable \| enable}`<br>`end` |

# Changes in GUI behavior

| Bug ID | Description |
|---|---|
| 780311 | The DLP profile is re-introduced in the GUI on the *Security Profiles* > *Data Leak Prevention* page. Users can configure DLP settings within the *Profiles*, *Sensors*, and *Dictionaries* tabs. DLP profiles can be added to proxy-based firewall policies and proxy policies. DLP profiles cannot be added to flow-based firewall policies and one-arm sniffers. |
| 805233 | The new *Log & Report* > *Reports* page consolidates *FortiAnalyzer*, *FortiGate Cloud*, and *Local* reports into a tab-based menu. The new *Log & Report* > *Log Settings* page consolidates the *Global Settings*, *Local Logs*, and *Threat Weight* settings into a tab-based menu. |

# Changes in default behavior

| Bug ID | Description |
|---|---|
| 780568 | Introduce CLI/WAD learn check for the same `url-map` among HTTPS, TCP forwarding, and SAML SP API gateway entities.<br>Before this change, the same `url-map` was allowed with different services. After this change, API gateway with the same `url-map` are not allowed under the same host (including empty vhosts).<br>If there is already a certain `url-map` configured in previous API gateways, under a certain vhost, then no more API gateways with the same `url-map` can be added under the same vhost. Users will get an error message stating this action is not allowed. |
| 819937 | For new firewall policies with a deny action, `set match-vip` is enabled by default. When upgrading from a previous version, existing policy settings for `match-vip` are preserved. |
| 829544 | Remove the maintainer account (which allowed users to log in through the console after a hard reboot). Users who lose their password must have physical access to the FortiGate and perform a TFTP restore of the firmware in order to regain access to the FortiGate. |

# Changes in default values

| Bug ID | Description |
|---|---|
| 798091 | Add speed option for 1000M auto-negotiation for FG-110xE. |
| 825537 | Change `voice-enterprise` default value from disable to enable. |
| 840537 | Change the default value of the `log-blocked-traffic` attribute of `firewall access-proxy` to be enabled. |

# Changes in table size

| Bug ID | Description |
|---|---|
| 823373 | Increase the number of VRFs per VDOM from 64 to 252. |
| 823708 | Increase the secondary IP limit from 32 to 256 addresses. |

# New features or enhancements

More detailed information is available in the New Features Guide.

| Bug ID | Description |
|---|---|
| 596988 | Support automatic vCPU hot add and hot remove to the limit of the license entitlements after activating an S-series license or a Flex-VM license. This enhancement removes the requirement for running the `execute cpu add <integer>` command or rebooting when the FortiGate VM has a lower number of vCPUs allocated than the licensed number of vCPUs. |
| 727383 | Add GUI support for IPv6 addresses in Internet Service Database (ISDB), and allow them to be configured in firewall policies. |
| 745172 | The information pane, which is located in the right-side gutter of many GUI pages, is enhanced to display the top three contextually appropriate questions as hyperlinks under the *Hot Questions at FortiAnswers* heading.<br>• Clicking a link takes the user to the related questions and answer page on the FortiAnswers website.<br>• The number of answers, votes, and views is displayed for each question.<br>• Clicking the *See more* link takes the user to the related topic page on FortiAnswers.<br>The existing documentation related links have been renamed:<br>• The *Documentation* section header is renamed to *Online Guides*.<br>• The *Online Help* link is renamed to *Relevant Documentation*. |
| 750073 | The `/api/v2/monitor/ips/session/performance` REST API can be used to query the FortiGate for its IPS session information. |
| 753177 | Display IoT devices with known vulnerabilities on the *Security Fabric* > *Asset Identity Center* page's *Asset* list view. Hovering over the vulnerabilities count displays a *View IoT Vulnerabilities* tooltip, which opens the *View IoT Vulnerabilities* table that includes the *Vulnerability ID*, *Type*, *Severity*, *Reference*, *Description*, and *Patch Signature ID*. Each entry in the *Reference* column includes the CVE number and a link to the CVE details.<br>The *Security Fabric* > *Security Rating* > *Security Posture* report includes *FortiGuard IoT Detection Subscription* and *FortiGuard IoT Vulnerability* checks. The *FortiGuard IoT Detection Subscription* rating check will pass if the *System* > *FortiGuard* page shows that the *IoT Detection Service* is licensed. The *FortiGuard IoT Vulnerability* rating check will fail if any IoT vulnerabilities are found.<br>To detect IoT vulnerabilities, the FortiGate must have a valid IoT Detection Service license, device detection must be configured on a LAN interface used by IoT devices, and a firewall policy with an application control sensor must be configured. |
| 763752 | Add GUI support for `ip6-delegated-prefix-iaid`. |
| 766646 | Enhance the *Security Fabric* > *Fabric Connectors* page to show a high-level overview of the Fabric components that are enabled and how they connect to each other. The *System* > *Fabric Management* page can be used to register and authorize Security Fabric devices instead of the using the Security Fabric network topology gutter, which has been removed from the *Security Fabric* > *Fabric Connectors* page. |

| Bug ID | Description |
|---|---|
| | Changes include:<br>• Improve the Security Fabric configuration settings to select the Security Fabric role.<br>• Merge relevant connectors into *Core Network Security Connectors* and *Security Fabric Connectors* sections.<br>  • The *Core Network Security Connectors* section includes the *Security Fabric Setup*, *LAN Edge Devices*, *Logging & Analytics*, and *FortiClient EMS* cards.<br>  • The *Security Fabric Connectors* section includes the *Central Management*, *Sandbox*, and *Supported Connectors* cards. |
| 766811 | Add support to allow the SSL VPN client to add source ranges for routing through an SSL interface.<br>`config vpn ssl client`<br>`  edit <name>`<br>`  set ipv4-subnets <subnets>`<br>`  set ipv6-subnets <subnets>`<br>`  next`<br>`end`<br>`config vpn ssl web portal`<br>`  edit <name>`<br>`  set client-src-range {enable \| disable}`<br>`  set ip-mode {range \| user-group \| dhcp \| no-ip}`<br>`  next`<br>`end` |
| 767570 | Add the Fabric Overlay Orchestrator, which is an easy-to-use GUI wizard within FortiOS that simplifies the process of configuring a self-orchestrated SD-WAN overlay within a single Security Fabric without requiring additional tools or licensing. Currently, the Fabric Overlay Orchestrator supports a single hub architecture and builds upon an existing Security Fabric configuration. This feature configures the root FortiGate as the SD-WAN overlay hub and configures the downstream FortiGates (first-level children) as the spokes. After configuring the Fabric Overlay, you can proceed to complete the SD-WAN deployment configuration by configuring SD-WAN rules. |
| 768062 | Add support to use FortiMonitor to detect link quality based on sending probes from behind the FortiGate for selected applications to measure additional values, such as network transmit time (NTT), server response time (SRT), and application errors (app_err).<br>`config system sdwan`<br>`  config health-check`<br>`  edit <name>`<br>`  set detect-mode agent-based`<br>`  next`<br>`  end`<br>`  config service`<br>`  edit <id>`<br>`  set agent-exclusive {enable \| disable}`<br>`  next`<br>`  end`<br>`end` |

| Bug ID | Description |
|---|---|
| 768458 | Add the ability to perform multi-processing for the wireless daemon (cw_acd) by allowing users to specify the `acd-process-count`. The count varies by model based on the number of FortiAPs it is allowed to manage.<br>`config wireless-controller global`<br>`  set acd-process-count <integer>`<br>`end` |
| 768966 | Before this enhancement, certificate-based authentication against Active Directory LDAP (AD LDAP) only supported the UserPrincipleName (UPN) as the unique identifier in the Subject Alternative Name (SAN) field in peer user certificates. This enhancement extends the use case to cover the RFC 822 Name (corporate email address) defined in the SAN extension of the certificate to contain the unique identifier used to match a user in AD LDAP. It also allows the DNS defined in the user certificate to be used as a unique identifier. |
| 773551 | The antivirus (AV) exempt list allows users to exempt known safe files that happen to be incorrectly classified as malicious by our AV signature and AV engine scan. By configuring an antivirus exempt list in the CLI, users can specify file hashes in MD5, SHA1, or SHA256 for matching, When matched, the FortiGate ignores the AV scan verdict so that the corresponding UTM behavior defined in the AV profile is not performed. The exempt list does not apply to results of outbreak prevention, machine learning, FortiNDR, or FortiSandbox inline scans. |
| 774766 | Add `server-cert` and `server-ca-cert` options for Symantec Endpoint Protection Manager (SEPM) SDN connectors, which allow users to specify a certificate or series of certificates for the FortiGate to trust when connecting to the SEPM server.<br>`config system sdn-connector`<br>`  edit <name>`<br>`  set server-cert <remote_certificate>`<br>`  set server-ca-cert <remote_or_CA_certificate>`<br>`  next`<br>`end` |
| 780571 | Add *Logs Sent Daily* chart for remote logging sources (FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud) to the *Logging & Analytics Fabric Connector* card within the *Security Fabric* > *Fabric Connectors* page and to the *Dashboard* as a widget for a selected remote logging source. |
| 795829 | Allow virtual patching to be applied to traffic destined to the FortiGate by applying IPS signatures to the local in interface using local in policies. Attacks geared towards GUI and SSH management access, for example, can be mitigated using IPS signatures pushed from FortiGuard, thereby virtually patching these vulnerabilities.<br>`config firewall local-in-policy`<br>`  edit <id>`<br>`  set virtual-patch {enable \| disable}`<br>`  next`<br>`end` |
| 801495 | Allow device statistics (bytes and packets) to be displayed on FortiGate when a FortiSwitch NAC policy is enabled. Statistics are collected per device/MAC address connected to FortiSwitch. |

| Bug ID | Description |
|---|---|
| | `# diagnose switch-controller telemetry show mac-stats switch <serial_number>` |
| 802001 | Add command to clean up old configurations, except for serial number and FortiManager IP, in `system.central-management`.<br>`# execute factoryreset-for-central-management` |
| 804870 | Add support to source the packets with the address of the client-facing interface instead of using the server-facing interface's address.<br>`config system interface`<br>`  edit <name>`<br>`  config ipv6`<br>`  set dhcp6-relay-source-interface {enable \| disable}`<br>`  end`<br>`  next`<br>`end` |
| 805565 | Add the `gui-proxy-inspection` setting under `config system settings`, which is enabled on most models except for low-end platforms with 2 GB of RAM or less. When this setting is disabled:<br>• Proxy-based only profiles such as *ICAP*, *Web Application Firewall*, *Video Filter*, and *Zero Trust Network Access* are disabled (grayed out) on the *System > Feature Visibility* page.<br>• The *Feature set* field is disabled on UTM profiles. Only flow-based features are shown.<br>• Firewall policy pages do not have option to select a *Flow-based* or *Proxy-based* inspection mode.<br>• Proxy-based UTM profiles cannot be selected within policy configurations or other areas.<br>Note the following exceptions:<br>• If the proxy feature set is enabled from the CLI or carried over from upgrading, it can be displayed in the GUI.<br>• If proxy-based inspection mode is enabled from the CLI or carried over from upgrading, it can be displayed in GUI firewall policy pages. |
| 805867 | Increase the number of supported NAC devices to 48 times the maximum number of FortiSwitch units supported on that FortiGate model. |

| Bug ID | Description |
|---|---|
| 806993 | Support ZTNA policy access control of unmanageable and unknown devices in the ZTNA application gateway by using the `EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` dynamic address local tags, respectively.<br>Enhance diagnostic commands:<br>• Use `diagnose firewall dynamic address` to view IP addresses of clients associated with `EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` dynamic addresses.<br>• Use `diagnose user-device-store device memory list` to view tags of devices identified through FortiGate device detection.<br>Enhance ZTNA traffic logs:<br>• The `emsconnection` (CLI) or *EMS Connection* (GUI) field is used for the client connection status with EMS server; possible values of unknown, offline, or online.<br>• The `clientdevicemanageable` (CLI) or *Client Device Manageable* (GUI) field is used for device manageability status.<br>In the GUI, tags can be specified in proxy policies (*Policy & Objects* > *ZTNA* > *ZTNA Rules*), and tags are visible on various pages (*Policy & Objects* > *ZTNA* > *ZTNA Tags*, *Dashboard* > *FortiClient* widget, and *Security Fabric* > *Asset Identity Center*). |
| 812120 | Support non-English keyboards for SSL VPN web mode with VNC by adding the `vnc-keyboard-layout` option for `config bookmarks` under `vpn ssl web portal`, `vpn ssl web user-bookmark`, and `vpn ssl web user-group-bookmark`. The server and client must have the same keyboard layout.<br>The available options are: `default`, `da` (Danish), `nl` (Dutch), `en-uk` (English, United Kingdom), `en-uk-ext` (English, United Kingdom Extended), `fi` (Finnish), `fr` (French), `fr-be` (French, Belgium), `fr-ca-mul` (French, Canadian multilingual standard), `de` (German), `de-ch` (German, Switzerland), `it` (Italian), `it-142` (Italian 142), `pt` (Portuguese), `pt-br-abnt2` (Portuguese Brazilian ABNT2), `no` (Norwegian), `gd` (Scottish Gaelic), `es` (Spanish), `sv` (Swedish), and `us-intl` (United States international). |
| 812993 | Support the blocking of a discovered FortiExtender device on a FortiGate configured as a FortiExtender controller using *Reject Status* in the GUI and `set authorized disable` in the CLI.<br>`config extension-controller extender`<br>`edit <name>`<br>`set id <string>`<br>`set authorized disable`<br>`next`<br>`end` |
| 813333 | Allow configuration of `interface-select-method` and `source-ip` for TACACS+ accounting servers. |
| 814796 | Remove the threat level threshold option from compromised host automation triggers in the GUI and CLI. |

| Bug ID | Description |
|---|---|
| 818343 | HTTP2 connection coalescing and concurrent multiplexing allows multiple HTTP2 requests to share the same TLS connection when the destination IP is the same and host names are compatible in the certificate. This is supported for ZTNA, virtual server load balancing, and explicit proxy. |
| 819508 | A FortiGate can allow single sign-on (SSO) from FortiCloud and FortiCloud IAM users with administrator profiles inherited from FortiCloud or overridden locally by the FortiGate. Similarly, users accessing the FortiGate remotely from FortiGate Cloud can have their permissions inherited or overridden by the FortiGate. |
| 819583 | Add guards to Node.JS log generation and move logs to `tmpfs` to prevent conserve mode issues. Node.JS logs only last a calendar day and will store up to 5 MB of logs. Once this limit is exceeded, the log file is deleted and a new file is created. A delete option has been added to the Node.JS debug command.<br>`# diagnose nodejs logs {list \| show <arg> \| show-all \| delete <arg>}` |
| 820902 | Add option to exclude the first and last IP of a NAT64 IP pool. This setting is enabled by default.<br>`config firewall ippool`<br>`edit <name>`<br>`set nat64 enable`<br>`set subnet-broadcast-in-ippool {enable \| disable}`<br>`next`<br>`end` |
| 820989 | Improve device identification of a router or proxy:<br>• Re-introduce the concept of router detection based on detecting the device type changing.<br>• Do not perform a signature check when scanning HTTP traffic if the headers contain `Via`, `Forwarded`, `X-Forwarded-For`, `X-Forwarded-Host`, or `X-Forwarded-Proto`.<br>• Modify the rules for TTL-based router detection. |
| 822249 | Add DHCP relay parameters under `config vpn ssl web portal` so user groups can get different scope IP addresses from the DHCP server.<br>`config vpn ssl web portal`<br>`edit <name>`<br>`set dhcp-ra-giaddr <gateway_IP_address>`<br>`set dhcp6-ra-linkaddr <IPv6_link_address>`<br>`next`<br>`end` |
| 822423 | Add option to support minimum and maximum version restrictions for the user agent.<br>`config firewall proxy-address`<br>`edit <name>`<br>`set type {src-advanced \| ua}`<br>`set ua <browser>`<br>`set ua-min-ver <string>`<br>`set ua-max-ver <string>`<br>`next`<br>`end` |

| Bug ID | Description |
|---|---|
| 823374 | BGP extended community route targets can be matched in route maps. This can be applied in a scenario where the BGP route reflector receives routes from many VRFs, and instead of reflecting all routes from all VRFs, users only want to reflect routes based on a specific extended community route target.<br>`config router extcommunity-list`<br>`edit <name>`<br>`set type {standard \| expanded}`<br>`config rule`<br>`edit <id>`<br>`set action {deny \| permit}`<br>`set type {rt \| soo}`<br>`set match <extended_community_specifications>`<br>`set regexp <ordered_list_of_attributes>`<br>`next`<br>`end`<br>`next`<br>`end`<br>`config router route-map`<br>`edit <name>`<br>`config rule`<br>`edit <id>`<br>`set match-extcommunity <list>`<br>`set match-extcommunity-exact {enable \| disable}`<br>`next`<br>`end`<br>`next`<br>`end` |
| 823702 | Allow VLAN sub-interfaces, such as regular 802.1Q and 802.1ad (QinQ), to be members of a virtual wire pair. |
| 823709 | Add TPM support for FG-VM64 platforms. Hypervisors with software TPM emulator packages installed will be able to support the TPM feature on FortiOS. This is currently supported on KVM and QEMU. |
| 823715 | Add support for independent upgrades of devices using sfupgraded.<br>• Add `coordinating` option for `status` attribute under `config system federated-upgrade`.<br>• Add `cancel` option to cancel a Fortinet device's upgrade by removing it from the upgrade table (`execute device-upgrade cancel <serial_number>`).<br>• Add immediate option to configure a Fortinet device to upgrade immediately (`execute device-upgrade immediate <device_type> <serial_number> <major> <minor> <patch>`).<br>• Add `system device-upgrade` table. This table is cannot be configured by the user.<br>`config system device-upgrade`<br>`edit <serial_number>` |

| Bug ID | Description |
|---|---|
| | <pre>set timing immediate<br>set setup-time 05:49 2022/07/26 UTC<br>set upgrade-path 7-0-5<br>set device-type fortiap<br>set status cancelled<br>set failure-reason device-missing<br>next<br>end</pre> |
| 823917 | Add option to set the IP fragment memory threshold manually (in MB, 32 - 2047, default = 32). A large memory threshold can reduce the number of ReasmFails due to the large number of fragment packets.<br><pre>config system global<br>set ip-fragment-mem-thresholds <integer><br>end</pre> |
| 825139 | Add option to embed a Base64 string instead of a plain text URL for images on the block pages.<br><pre>config webfilter fortiguard<br>set embed-image {enable \| disable}<br>end</pre> |
| 825308 | Allow FortiGate-VMs for OCI to work on ARM-based Oracle Cloud Ampere A1 Compute instances. |
| 825951 | Add the ability for Dynamic ARP Inspection (DAI) to examine ARP packets against static clients with static IP-MAC binding. Configurations can be pushed by the FortiGate switch controller to managed switches.<br><pre>config switch-controller managed-switch<br>edit <serial_number><br>config dhcp-snooping-static-client<br>edit <name><br>set ip <IP_address><br>set vlan <vlan_ID><br>set mac <MAC_address><br>set port <port><br>next<br>end<br>next<br>end</pre> |
| 827460 | Allow users to specify cloud mode in the user data during deployment to insert a `Cloud mode: cnf` identification in the `get system status` output. This allows FortiManager to detect the managed FortiGate as a FortiGate-CNF device and disable certain settings. |
| 829458 | Remove the `allow-quic` option from the `options` setting under `config application list`. The *QUIC* option is also removed from the *Application Sensor* configuration page in the GUI. Since HTTP3 over QUIC is fully supported by FortiOS, blocking QUIC by default in the application control profile is no longer necessary. |

| Bug ID | Description |
|---|---|
| 829628 | Add option for matching IPv4 mapped IPv6 URLs. This setting is disabled by default. When enabled, if the URL filter entry's URL hostname is an IPv4 address, the URL filter list will build an extra entry with the mapped IPv6 hostname URL This is the same URL as the original URL, except that the hostname is replaced with the mapped IPv6 hostname.<br>`config webfilter urlfilter`<br>`edit <id>`<br>`set ip4-mapped-ip6 {enable \| disable}`<br>`next`<br>`end` |
| 830527 | Added option to set the VRF route on a VPN interface with `vpn-id-ipip` encapsulation. Previously, VRFs in static routes could only be set if the blackhole was enabled.<br>`config router static`<br>`edit <seq-num>`<br>`set device "vpn1"`<br>`set vrf 1`<br>`next`<br>`end`<br>BFD is skipped when the VPN interface uses `vpn-id-ipip` encapsulation. |
| 831010 | Support wireless client mode on FortiWiFi 80F series models. When wireless client mode is successfully configured, a default static route to the `aplink` interface is automatically created. For outgoing traffic using this wireless client connection, a firewall policy from the wired internal/LAN interface as the source interface to the `aplink` interface as the destination interface must be configured. |
| 831427 | Add `log-single-cpu-high` option under `config system global`. When enabled, CPU single core usage will be polled every three seconds, and any single CPU core usage above the CPU usage threshold will report an event log. If a core is reported, that core will not be checked again for the next 30 seconds.<br>`config system global`<br>`set log-single-cpu-high {enable \| disable}`<br>`end` |
| 831492 | Add support to allow individual FortiGates in the Security Fabric to have their own automation setting.<br>`config automation setting`<br>`set fabric-sync {enable \| disable}`<br>`end` |
| 832041 | Add options to filter WAD log messages by process type or process ID, and print WAD log messages by default when the session is unknown.<br>`# diagnose wad filter process-type <integer>`<br>`# diagnose wad filter process-id <integer>` |

| Bug ID | Description |
|---|---|
| | When running `diagnose wad filter list`, the `process type` and `process id` are visible in the output. |
| 832435 | Add support for PoE mode, power, and priority switch port options on FortiSwitch through the switch controller for supported models.<br>`config switch-controller managed-switch`<br>`edit <switch-id>`<br>`config ports`<br>`edit <name>`<br>`set poe-port-mode {ieee802-3af \| ieee802-3at}`<br>`set poe-port-priority {critical-priority \| high-priority \| low-priority}`<br>`set poe-port-power {normal \| perpetual \| perpetual-fast}`<br>`next`<br>`end`<br>`next`<br>`end` |
| 833111 | Add option to enable or disable rewriting the `Host` field in HTTP requests through a virtual server or access proxy before being sent to a real server.<br>`config firewall vip`<br>`edit <vip>`<br>`set type server-load-balance`<br>`config realservers`<br>`edit <id>`<br>`set translate-host {enable \| disable}`<br>`next`<br>`end`<br>`next`<br>`end`<br>`config firewall access-proxy`<br>`edit <name>`<br>`config api-gateway`<br>`edit <id>`<br>`config realservers`<br>`edit <id>`<br>`set translate-host {enable \| disable}`<br>`next`<br>`end`<br>`next`<br>`end`<br>`next`<br>`end` |
| 834861 | Add route tags to static routes.<br>`config router static` |

| Bug ID | Description |
|---|---|
| | ```<br>edit <seq-num><br>set tag <id><br>next<br>end<br>```<br>Add password field to BGP neighbor group to be used for the neighbor range.<br>```<br>config router bgp<br>config neighbor-group<br>edit <name><br>set password <password><br>next<br>end<br>end<br>``` |
| 836287 | Support adding YAML to the file name when backing up the config as YAML, and detecting file format when restoring the configuration.<br>The `execute restore yaml-config` command has been removed and `execute restore config` should be used.<br>In the GUI, the *File format* field has been removed from the *Restore system Configuration* page. |
| 836613 | Add option for each FortiClient EMS connector (`trust-ca-cn`). This option is enabled by default. When enabled, the CA and CN information is stored with the connector, which allows the FortiGate to automatically approve an updated certificate so long as it has the same CA and CN.<br>```<br>config endpoint-control fctems<br>edit <id><br>set trust-ca-cn {enable \| disable}<br>next<br>end<br>``` |
| 836653 | Add commands to list the NPU session summary.<br>```<br># diagnose sys npu-session list-brief<br>```<br>```<br># diagnose sys npu-session list-brief6<br>``` |
| 836851 | Enhance DHCP:<br>• Increase the number of supported IP ranges from 3 to 10<br>• Support DHCP option 77 for User Class information<br>• Support customizing the lease time per IP range (CLI only) |
| 838363 | Internet Service Database (ISDB) on-demand mode replaces the full-sized ISDB file with a much smaller file that is downloaded onto the flash drive. This file contains only the essential entries for Internet Services. When a service is used in a firewall policy, the FortiGate queries FortiGuard to download the IP addresses and stores them on the flash drive. The FortiGate also queries the local MAC Database (MADB) for corresponding MAC information.<br>```<br>config system global<br>set internet-service-database on-demand<br>end<br>``` |

| Bug ID | Description |
|---|---|
| 839877 | FortiPolicy can be added to the Security Fabric. When FortiPolicy joins the Security Fabric and is authorized in the *Security Fabric* widget, it appears in the Fabric topology pages. A FortiGate can grant permission to FortiPolicy to perform firewall address and policy changes. Two security rating tests for FortiPolicy have been added to the *Security Posture* scorecard. |
| 839951 | Add FGT-ARM64-GCP image to support ARM64-based GCP VMs of the GCP Tau T2A instance family. |
| 841928 | In some scenarios where it is necessary to simulate a system crash, the following commands allow a super_admin administrator to safely trigger a kernel crash using a SysRq key.<br>`# diagnose debug kernel sysrq status`<br>`# diagnose debug kernel sysrq {enable \| disable}`<br>`# diagnose debug kernel sysrq command crash`<br>A kernel crash dump is outputted to the console. The FortiGate reboots and recovers without losing any functionality. This is only supported on FortiGate VMs. |
| 841934 | Enhance the FortiGate AWS SDN connector to resolve various AWS endpoint ENI IP addresses:<br>• API Gateway private endpoints<br>• VPC endpoints for Aurora Data API<br>• AWS PrivateLink for S3<br>• VPC endpoints for Lamdba<br>This adds support for dynamic policies in FortiGate CNF, and to resolve various AWS PrivateLink endpoints for dynamic policies in typical deployments. |
| 844039 | When WAN-LAN operation and LAN port options are configured on the FortiGate and FortiAP, the FortiGate can display details about wired clients connected to the FortiAP LAN port in each of the following cases:<br>• LAN2 port of FortiAP models with LAN1 and LAN2 ports<br>• LAN port of FortiAP models with LAN and WAN ports<br>The following configuration settings are required:<br>• WAN-LAN operation must be configured using `set wan-port-mode wan-lan` on the FortiGate's FortiAP profile and `cfg -a WANLAN_MODE=WAN-LAN` using the FortiAP CLI, respectively.<br>• LAN port mode can be configured using any of the `port-mode` options (`nat-to-wan`, `bridge-to-wan`, `bridge-to-ssid`) under `config lan` within `config wireless-controller wtp-profile`.<br>Details about wired clients are displayed in the FortiOS CLI using `diagnose wireless-controller wlac -c lan-sta`, and in the FortiAP CLI using `cw_diag -c k-lan-host`. |
| 849771 | Support Shielded and Confidential VM modes on GCP where the UEFI VM image is used for secure boot, and data in use is encrypted during processing. |
| 855684 | Allow users to configure the RADIUS NAS-ID as a custom ID or the hostname. When deploying a wireless network with WPA-Enterprise and RADIUS authentication, or using the RADIUS MAC authentication feature, the FortiGate can use the custom NAS-ID in its Access-Request.<br>`config user radius` |

| Bug ID | Description |
|---|---|
| | `edit <name>`<br>`set nas-id-type {legacy \| custom \| hostname}`<br>`set nas-id <string>`<br>`next`<br>`end` |
| 858786 | When configuring a CGN IP pool for a hyperscale firewall, exclude IP addresses within this IP pool from being used for source NAT (`excludeip`). This allows users to remain secure and mitigate attacks by ensuring that global IP addresses within a CGN IP pool that are being targeted by external attackers are not re-used by other users of the hyperscale firewall.<br>`config firewall ippool`<br>`edit <name>`<br>`set type cgn-resource-allocation`<br>`set startip <IPv4_address>`<br>`set endip <IPv4_address>`<br>`set excludeip <IPv4_address>, <IPv4_address>, <IPv4_address> ...`<br>`next`<br>`end`<br>This option is currently not supported with a fixed allocation CGN IP pool (when `set cgn-fixedalloc enable` is configured). |

# Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

**To view supported upgrade path information:**

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

## Fortinet Security Fabric upgrade

FortiOS 7.2.4 greatly increases the interoperability between other Fortinet products. This includes:

| | |
|---|---|
| **FortiAnalyzer** | • 7.2.1 |
| **FortiManager** | • 7.2.1 |
| **FortiExtender** | • 4.0.0 and later. For compatibility with latest features, use latest 7.0 version. |
| **FortiSwitch OS (FortiLink support)** | • 6.4.6 build 0470 or later |
| **FortiAP**<br>**FortiAP-S**<br>**FortiAP-U**<br>**FortiAP-W2** | • See Strong cryptographic cipher requirements for FortiAP on page 29 |
| **FortiClient* EMS** | • 7.0.3 build 0229 or later |
| **FortiClient* Microsoft Windows** | • 7.0.3 build 0193 or later |
| **FortiClient* Mac OS X** | • 7.0.3 build 0131 or later |
| **FortiClient* Linux** | • 7.0.3 build 0137 or later |
| **FortiClient* iOS** | • 7.0.2 build 0036 or later |
| **FortiClient* Android** | • 7.0.2 build 0031 or later |
| **FortiSandbox** | • 2.3.3 and later for post-transfer scanning<br>• 4.2.0 and later for post-transfer and inline scanning |

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.4. When Security Fabric is enabled in FortiOS 7.2.4, all FortiGate devices must be running FortiOS 7.2.4.

# Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

# Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

# FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, Flex-VM) have a maximum number or two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0. After upgrading to 7.2.0, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

# Product integration and support

The following table lists FortiOS 7.2.4 product integration and support information:

| | |
|---|---|
| **Web browsers** | • Microsoft Edge<br>• Mozilla Firefox version 105<br>• Google Chrome version 109<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **Explicit web proxy browser** | • Microsoft Edge 44<br>• Mozilla Firefox version 74<br>• Google Chrome version 80<br>Other web browsers may function correctly, but are not supported by Fortinet. |
| **FortiController** | • 5.2.5 and later<br>Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C |
| **Fortinet Single Sign-On (FSSO)** | • 5.0 build 0308 and later (needed for FSSO agent support OU in group filters)<br>  • Windows Server 2022 Standard<br>  • Windows Server 2019 Standard<br>  • Windows Server 2019 Datacenter<br>  • Windows Server 2019 Core<br>  • Windows Server 2016 Datacenter<br>  • Windows Server 2016 Standard<br>  • Windows Server 2016 Core<br>  • Windows Server 2012 Standard<br>  • Windows Server 2012 R2 Standard<br>  • Windows Server 2012 Core<br>  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)<br>  • Windows Server 2008 Core (requires Microsoft SHA2 support package)<br>  • Novell eDirectory 8.8 |
| **AV Engine** | • 6.00285 |
| **IPS Engine** | • 7.00255 |

## Virtualization environments

The following table lists hypervisors and recommended versions.

| Hypervisor | Recommended versions |
|---|---|
| **Citrix Hypervisor** | • 8.1 Express Edition, Dec 17, 2019 |
| **Linux KVM** | • Ubuntu 18.0.4 LTS<br>• Red Hat Enterprise Linux release 8.4<br>• SUSE Linux Enterprise Server 12 SP3 release 12.3 |
| **Microsoft Windows Server** | • 2012R2 with Hyper-V role |
| **Windows Hyper-V Server** | • 2019 |
| **Open source XenServer** | • Version 3.4.3<br>• Version 4.1 and later |
| **VMware ESXi** | • Versions 6.5, 6.7, and 7.0. |

# Language support

The following table lists language support information.

**Language support**

| Language | GUI |
|---|---|
| English | ✓ |
| Chinese (Simplified) | ✓ |
| Chinese (Traditional) | ✓ |
| French | ✓ |
| Japanese | ✓ |
| Korean | ✓ |
| Portuguese (Brazil) | ✓ |
| Spanish | ✓ |

# SSL VPN support

## SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

**Supported operating systems and web browsers**

| Operating System | Web Browser |
|---|---|
| Microsoft Windows 7 SP1 (32-bit & 64-bit) | Mozilla Firefox version 105<br>Google Chrome version 109 |
| Microsoft Windows 10 (64-bit) | Microsoft Edge<br>Mozilla Firefox version 105<br>Google Chrome version 109 |
| Ubuntu 20.04 (64-bit) | Mozilla Firefox version 105<br>Google Chrome version 109 |
| macOS Monterey 12.2 | Apple Safari version 15<br>Mozilla Firefox version 98<br>Google Chrome version 99 |
| iOS | Apple Safari<br>Mozilla Firefox<br>Google Chrome |
| Android | Mozilla Firefox<br>Google Chrome |

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

# Resolved issues

The following issues have been fixed in version 7.2.4. To inquire about a particular bug, please contact Customer Service & Support.

## Anti Spam

| Bug ID | Description |
|---|---|
| 857911 | The *Anti-Spam Block/Allow List Entry*dialog page is not showing the proper *Type* values in the dropdown. |

## Anti Virus

| Bug ID | Description |
|---|---|
| 727067 | FortiGate should fix the interface between FortiGate and FortiAnalyzer for the CDR file. |
| 794575 | If FortiGate Cloud is selected as sandbox server under *Security Fabric* > *Fabric Connectors*, an anti virus profile with settings to *Send files to FortiSandbox for inspection* does not get saved in the GUI. |
| 800731 | Flow AV sends HTML files to the FortiGate Cloud Sandbox every time when HTML is not configured in file list. |
| 818092 | CDR archived files are deleted at random times and not retained. |
| 823677 | When a FortiGate with DLP patterns configured is connected to FortiSandbox, scanunit crashes when the FortiSandbox extension reloads or worker shuts down. |
| 845960 | Flow mode opens port 8008 over the AV profile that does not have HTTP scan enabled. |
| 849020 | FortiGate enters conserve mode and the console prints a `fork()` failed message. |

## Application Control

| Bug ID | Description |
|---|---|
| 829458 | Remove option to block QUIC by default. |

## Data Leak Prevention

| Bug ID | Description |
|---|---|
| 828621 | DLP is not blocking files larger than the threshold value defined in `set file-size`. |

## Endpoint Control

| Bug ID | Description |
|---|---|
| 817140 | Device is constantly unauthorized in EMS when using `set interface-select-method sdwan`. |
| 834168 | FortiGates get deauthorized on EMS. |

## Explicit Proxy

| Bug ID | Description |
|---|---|
| 803228 | When converting an explicit proxy session to SSL redirect and if this session already has connected to an HTTP server, the WAD crashes continuously with signal 11. |
| 805703 | FortiGate does not load balance requests evenly when the `ldb-method` is set to `least-session`. |
| 823319 | Authentication hard timeout is not respected for firewall users synchronized from WAD user. |

## Firewall

| Bug ID | Description |
|---|---|
| 631814 | *Static route configuration* should not be shown on address dialog page if the address type is an IP range. |
| 728734 | The VIP group hit count in the table (*Policy & Objects* > *Virtual IPs*) is not reflecting the correct sum of VIP members. |
| 784766 | When a FortiGate virtual server for Exchange incorrectly indicates to the Exchange server that it does not support secure renegotiation when it should, the Exchange server terminates the connection and returns an `ERR_EMPTY_RESPONSE`. |
| 800730 | When using NGFW policy-based mode, modifying a security policy causes all sessions to be reset. |

| Bug ID | Description |
|---|---|
| 808264 | Stress test shows packet loss when testing with flow inspection mode and application control. |
| 815565 | Unable to connect to the reserved management interface allowed by the local-in policy. |
| 823917 | Packet loss occurs due to a high amount of fragment reassembly failures. |
| 824091 | Promethean Screen Share (multicast) is not working on the member interfaces of a software switch. |
| 827780 | ISDB source matching is inconsistent between transparent and NAT modes. |
| 829071 | Geolocation block on VIP object failed with seemly correct configuration. |
| 829664 | Kernel panic occurs while collecting the debug flow. |
| 830823 | Traffic is dropped intermittently by the implicit deny policy, even though there is a valid policy on the FortiGate. |
| 832217 | Traffic is hitting the implicit deny policy when changes are made to a policy. |
| 834301 | Session dropped with timeout action after policy changes. |
| 835413 | Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0. |
| 840689 | Virtual server aborts connection when `ssl-max-version` is set to `tls-1.3`. |
| 843274 | Source interface filter (`srcintf-filter`) is not working with virtual servers. |
| 847086 | Unable to add additional MAC address objects in an address group that already has 152 MAC address objects. |
| 852714 | Making a full HTTP session is sometimes bypassed if `ssl-hsts` is enabled for a `server-load-balance` VIP. |
| 865661 | Standard and full ISDB sizes are not configurable on FG-101F. |

## FortiView

| Bug ID | Description |
|---|---|
| 798427 | Change the sandbox PDF report query to be on-demand. |
| 838652 | The *FortiView Sessions* monitor displays VDOM sessions from other VDOMs. |

# GUI

| Bug ID | Description |
|---|---|
| 440197 | On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly. |
| 712414 | On the *System* > *Fabric Management* page, the registration status for FortiSwitches and FortiAPs have a *Failed to fetch status* error. |
| 719476 | FortiLink NAC matched device is displayed in the CLI but not in the GUI under *WiFi & Switch Controller* > *NAC Policies* > *View Matched Devices*. |
| 722358 | When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode. |
| 729406 | New IPsec design `tunnel-id` still displays the gateway as an IP address, when it should be a tunnel ID. |
| 749843 | *Bandwidth* widget does not display traffic information for VLAN interfaces when a large number of VLAN interfaces are configured. |
| 780832 | *WiFi & Switch Controller* > *Managed FortiAPs* list does not load if there is an invalid or unsupported FortiAP configured. |
| 794656 | After rebooting, the *Licenses* widget shows an `Unable to connect to FortiGuard servers` message for ten minutes. |
| 794757 | Inbound traffic on the interface bandwidth widget shows *0 bps* on the VLAN interface. |
| 804584 | On the policy dialog page, the *Select Entries* box for the *Service* field does not list all service objects if an IPv6 address is in the policy. |
| 807197 | High `iowait` CPU usage and memory consumption issues caused by report runner. |
| 819272 | When a VLAN belongs to a zone, and the zone is used in a policy, editing the VLAN ID changes the policy's position in the table. |
| 820909 | On the *Policy & Objects* > *Schedules* page, when the end date of a one-time schedule is set to the 31st of a month, it gets reset to the 1st of the same month.<br>**Workaround**: use CLI to set schedules with an end date of 31st. |
| 821030 | Security Fabric root FortiGate is unable to resolve firewall object conflicts in the GUI. |
| 821734 | *Log & Report* > *Forward Traffic* logs do not show the *Policy ID* if there is no *Policy Name*. |
| 822991 | On the *Log & Report* > *Forward Traffic* page, using the filter *Result : Deny(all)* does not work as expected. |
| 825377 | *Managed FortiSwitches* page, policy pages, and some FortiView widgets are slow to load. |
| 827893 | Security rating test result incorrectly shows *Failed* for FortiManager Cloud FortiCare support. |
| 829313 | The dropdown field for the IdP *Certificate* is empty when editing an SSO user configuration (*User & Authentication* > *Single Sign-On*), even though the summary shows an IdP certificate. |

| Bug ID | Description |
|---|---|
| 829736 | Incorrect information is being displayed for the HA role on the *System* > *HA* page. |
| 829773 | Unable to load the *Network* > *SD-WAN* > *SD-WAN Rules* table sometimes due to a JavaScript error. |
| 831439 | On the *WiFi & Switch Controller* > *SSIDs* page, multiple DHCP servers for the same range can be configured on an interface if the interface name contains a comma (,) character. |
| 831885 | Unable to access GUI via HA management interface of secondary unit. |
| 833306 | Intermittent error, *Failed to retrieve FortiView data*, appears on real-time *FortiView Sources* and *FortiView Destination* monitor pages. |
| 833774 | GUI needs to allow the members of the software switch interface to be used in IPv4/IPv6 multicast policy. |
| 835089 | Unable to move SD-WAN rule ordering in the GUI (FortiOS 7.2.1). |
| 837836 | The *Network* > *Interfaces* faceplate shows two SFP interfaces, which do not exist on that FortiGate model. |
| 840604 | When upgrading the FortiGate firmware upgrade from FortiGuard, update the API description text for the file name. |
| 842079 | On the *System* > *HA* page, a *Failed to retrieve info* caution message appears when hovering over the secondary unit's *Hostname*. The same issue is observed on the *Dashboard* > *Status* > *Security Fabric* widget. |
| 845513 | On G-model profiles, changing the platform mode change from single 5G (dedicated scan enabled) to dual 5G is not taking effect. |
| 854529 | The local standalone mode in a VAP configuration is disabled when viewing or updating its settings in the GUI. |

## HA

| Bug ID | Description |
|---|---|
| 738728 | The secondary unit tries to contact the forward server for sending the health check packets when the `healthcheck` under `web-proxy forward-server` is enabled. |
| 777394 | Long-lasting sessions expire on the HA secondary in large session synchronization scenarios. |
| 788702 | Due to an HA port (Intel i40e) driver issue, not all SW sessions are synchronized to the secondary, so there is a difference. |
| 813207 | Virtual MAC address is sent inside GARP by the secondary unit after a reboot. |
| 818432 | When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures. |
| 819872 | HA split brain scenario occurs after upgrading from 6.4.6 to 7.0.6, and HA heartbeats are lost followed by a kernel panic. Affected platforms: NP7 models. |

| Bug ID | Description |
|---|---|
| 823687 | A cluster is repeatedly out-of sync due to external files (SSLVPN_AUTH_GROUPS) when there are frequent user logins and logouts. |
| 824200 | HA is out-of-sync due to SD-WAN default configuration for a newly created VDOM. |
| 824651 | Certificate upload causes HA checksum mismatch. |
| 826188 | Secondary FortiGate FQDN is stuck in the queue, even if the primary FortiGate FQDN has already been resolved. |
| 829390 | When the internet service name management checksum is changed, it is out-of-sync when the auto-update is disabled on FortiManager. |
| 830463 | After shutting down the HA primary unit and then restarting it, the uptime for both nodes is zero, and it fails back to the former primary unit. |
| 830879 | Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list. |
| 832634 | HA failovers occur due to the kernel hanging on FG-100F. |
| 835331 | Communication is disrupted when HA switching is performed in an environment where the VDOM is split to accommodate two IPoE lines. |
| 837888 | CLI deployment of a configuration to the secondary unit results in an unresponsive aggregate interface. |
| 838571 | After an HA split-brain event, the PPPoE interfaces are not recovered. |
| 839549 | Secondary FortiGate unit in an HA cluster enters conserve mode due to high memory consumption by node scripts. |
| 840305 | Static ARP entry is removed after reboot or HA failover. |
| 840954 | The HA pair primary keeps sending `fgFmTrapIfChange` and `fnTrapIpChange` after upgrading. |
| 843837 | HA A-P virtual cluster information is not correctly presented in the GUI and CLI. |
| 843907 | Session load balancing is not working in HA A-A configuration for traffic flowing via the VLAN interface when the port1 link is down on platforms with a 4.19 kernel. |
| 846015 | The first ICMP redirected from the FGSP secondary is dropped on the FGSP primary when UTM is enabled. |

# Hyperscale

| Bug ID | Description |
|---|---|
| 771857 | VIP port forwarding (`src-filter`) does not work in a hyperscale policy. |

| Bug ID | Description |
|---|---|
| 804742 | After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions. |
| 807476 | After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled. |
| 824733 | IPv6 traffic continues to pass through a multi-VDOM setup, even when the static route is deleted. |
| 835697 | Interface routes under DHCP mode remain in LPMD after moving the interface to another VDOM. |
| 836474 | Changes in the zone configuration are not updated by the NPD on hyperscale. |
| 837270 | Disabling *Block intra-zone traffic* in a zone does not allow TCP/UDP traffic between interfaces of a zone. |
| 843305 | Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up. |

## ICAP

| Bug ID | Description |
|---|---|
| 832515 | Bad gateway occurs using ICAP with explicit proxy under traffic load. |

## Intrusion Prevention

| Bug ID | Description |
|---|---|
| 695464 | High IPS engine CPU usage due to recursive function call. |
| 755859 | The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode. |
| 771000 | High CPU in all cores with device running with one interface set as a one-arm sniffer. |
| 809691 | High CPU usage on IPS engine when certain flow-based policies are active. |
| 848003 | FG-200E memory is not released and enters conserve mode, even after the traffic stopped. |

# IPsec VPN

| Bug ID | Description |
|---|---|
| 757696 | Implementing the `route-overlap` setting on phase 2 configurations brings tunnels down until a reboot is not performed on the FGSP cluster. |
| 763205 | IKE crashes after HA failover when the `enforce-unique-id` option is enabled. |
| 765174, 775279 | Certain packets are causing IPsec tunnel drops on NP6XLite platforms after HA failover because the packet is not checked properly. |
| 765868 | The packets did not pass through QTM, and SYN packets bypass the IPsec tunnel once traffic is offloaded. Affected platforms: NP7 models. |
| 798045 | FortiGate is unable to install SA (`failed to add SA, error 22`) when there is an overlap in configured selectors. |
| 805301 | Enabling NPU offloading in the phase 1 settings causes a complete traffic outage after a couple of ping packets pass through. |
| 807086 | ADVPN hub randomly initiates secondary tunnel to spoke, causing spoke to drop tunnel traffic for RPF check fail. |
| 815253 | NP7 offloaded egress ESP traffic that was not sent out of the FortiGate. |
| 819276 | After changing the password policy to enable it, all non-conforming IPsec tunnels were wiped out after rebooting/upgrading. |
| 822651 | NP dropping packet in the incoming direction for FG-200F. |
| 824532 | IPsec learned route disappears from the routing table. |
| 825523 | NP7 drops outbound ESP after IPsec VPN is established for some time. |
| 827350 | Dialup selector routes are not deleted after iked crash. |
| 828467 | IKE repeatedly crashes with the combination of DDNS and dialup gateways. |
| 828541 | IPsec DPD packets keep getting sent while IPsec traffic passes through the tunnel (DPD mode is `on-idle`). |
| 829091 | The iked daemon experiences a signal 11 crash when a static IPsec gateway is configured, the FortiGates are in HA, and an HA state change occurs. |
| 829939 | Unable to send traffic in VXLAN over IPSec when the VTEP is configured in a VDOM. |
| 830252 | IPsec VPN statistics are not increasing on the device. |
| 832920 | Unable to edit the parent interface from the IPsec configuration if it was configured on an IPIP tunnel. |
| 836260 | The IPsec aggregate interface does not appear in the *Interface* dropdown when configuring the *Interface Bandwidth* widget. |
| 840006 | A new VPN interface with `vpn-id-ipip` encapsulation has MAC address ff:ff:ff:ff:ff:ff and cannot set remote the IP until the FortiGate reboots. |

| Bug ID | Description |
|---|---|
| 840153 | Unexpected dynamic selectors block traffic when `set mesh-selector-type subnet` is configured. |
| 840940 | Unable to reestablish a new IPsec L2TP connection for 10 minutes after the previous one disconnected. The issue conditions are local in traffic and a policy-based IPsec tunnel. |
| 842528 | Improper IKEv1 quick mode fragmentation from third-party client can cause an IKE crash. |
| 846361 | OCVPN fails to create a policy when the interface belongs to a zone. |

## Log & Report

| Bug ID | Description |
|---|---|
| 789007 | Unable to select FortiAnalyzer as a data source on the *Summary* tab for the *System Events* and *Security Events* pages. |
| 814758 | Get an intermittent error when running `execute log fortianalyzer-cloud test-connectivity`. |
| 820940 | On the *Log Settings* page, a VDOM administrator can force a FortiCloud log out of for all VDOMs. |
| 821359 | FortiGate appears to have a limitation in the syslogd filter configuration. |
| 821494 | Forward traffic logs intermittently fail to show the destination hostname. |
| 826431 | FortiGate Cloud log viewer shows no results for the *5 minutes* and *1 hour* time period due to an incorrect timestamp (*24 hours* is OK). |
| 826483 | The `dstname` log field cannot store more than 66 characters. |
| 828211 | Policy ID filter is not working as expected. |
| 829862 | On the *Log & Report* > *ZTNA Traffic* page, the client's *Device* ID is shown as *[object Object]*. The Log Details pane show the correct ID information. |
| 836846 | Packet captured by firewall policy cannot be downloaded. |
| 837116 | FortiCloud log statistics chart on the *Log Settings* page shows incorrect data. |
| 838253 | FortiAnalyzer log statistics chart on the *Log Settings* page shows incorrect data. |
| 839601 | Unable to view logs longer than 500 lines by scrolling down or using the drag down function. |
| 847213 | Unable to mouse over an IP address in FortiGate logs. |
| 850519 | *Log & Report*> *Forward Traffic* logs do not return matching results when filtered with *!<application name>*. |
| 858304 | When FortiGate Cloud logging is enabled, the option to display *7 days* of logs is not visible on the FortiView pages. |
| 858589 | Unable to download more than 500 logs from the FortiGate GUI. |

# Proxy

| Bug ID | Description |
|---|---|
| 745701 | An issue occurs with TLS 1.3 and the 0RTT process where Firefox cannot access https.google.com using proxy-based UTM with certification inspection. |
| 780182 | WAD crash occurred when forwarding the release bytes from the IPS engine to the server and the connection to the server is closed. |
| 793651 | An expired certificate can be chosen when creating an SSL/SSH profile for deep inspection. |
| 795360 | Apple push notification service fails with proxy-based inspection. |
| 797620 | HTTPS sites blocked due to `cert-probe-failed` triggered by SSL exemption in deep inspection. |
| 799237 | WAD crash occurs when TLS/SSL renegotiation encounters an error. |
| 799381 | WAD crash occurs when TLS 1.2 receives the client certificate and that server-facing SSL port has been closed due to the SSL bypass. |
| 803286 | Inspecting all ports in deep inspection is dependent on previous protocol port mapping settings. |
| 808831 | Upgrading broke IM controls and caused Zalo chat file transfer issues. |
| 810792 | WAD crashes when the following conditions are met: the FortiGate is an HA secondary, it is configured with a web proxy forward server in a proxy policy, and the forward server has health check enabled. |
| 813562, 823247, 823829, 829428 | When an LDAP user is authenticated in a firewall policy, the WAD user-info process has a memory leak causing the FortiGate to enter conserve mode. |
| 814061 | Stress test shows cryptographic errors in proxy mode. |
| 818371 | WAD process crashes with some URIs. |
| 823814 | Found WAD crash at signal 11 on `wad_http_engine.c` when `ap.empty-cert-action` is set to `accept-unmanageable`. |
| 825496 | Explicit proxy traffic is terminated when IPS is enabled. The exact failure happened upon certificate inspection. |
| 827882 | One WAD daemon is consistently using 99% CPU. |
| 830166 | When WAN optimization is disabled and the dispatcher sends the tunnel manager listener to the workers, the workers cannot handle it properly and a WAD crash segmentation fault occurs. |
| 830450 | Changing the virtual server configuration during traffic caused the old configuration to flush, which resulted in a WAD crash. |
| 830907 | WAD crash occurs when configuring a proxy policy with no member in an address group. |
| 834314 | ICAP client timeout issue causes WAD segmentation fault crash after upgrading to 7.0.6 from 6.4. |

| Bug ID | Description |
|---|---|
| 834998 | TLS 1.3 handshake fails in proxy mode when the FortiGate tries to obtain certificate information from a specific server. |
| 835903 | There is no replacement message for an IPS custom signature block in a proxy inspection mode firewall policy or proxy policy. |
| 836198 | Console randomly displays a `read_tagbuf - 152: Failed to open device: /dev/sdb errno:2(No such file or directory)` error. |
| 857368 | WAD crash with signal 11 caused by a stack allocated buffer overflow when parsing Huffman-encoded HTTP header name if the header length is more than 256 characters. |

## REST API

| Bug ID | Description |
|---|---|
| 836760 | The `start` parameter has no effect with the `/api/v2/monitor/user/device/query` API call. |
| 847526 | Able to add incomplete policies with empty mandatory fields using the REST API. |

## Routing

| Bug ID | Description |
|---|---|
| 769330 | Traffic does not fail over to alternate path upon interface being down (FGR-60F in transparent mode). |
| 819674 | Virtual server active-standby failover is not working with a UDP server type. |
| 822659 | *Secure SD-WAN Monitor* in FortiAnalyzer does not show graphs when the SLA target is not configured in SD-WAN performance SLA. |
| 823293 | Disabling BFD causes an OSPF flap/bounce. |
| 828121 | In a BGP neighbor, the `allowas-in 0` value is confusing and not accepted by the GUI for validation (1-10 required). |
| 828345 | Wrong MAC address is in the ARP response for VRRP IP instead of the VRRP virtual MAC. |
| 828780 | Router prefix list matching is not work properly for VPNv4 routes. |
| 830254 | When changing interfaces from dense mode to sparse mode, and then back to dense mode, the interfaces did not show up under dense mode. |
| 833399 | Static routes are incorrectly added to the routing table, even if the IPsec tunnel type is static. |
| 833800 | The `speed-test-server` list cannot be loaded due to limited buffer size. |

| Bug ID | Description |
|---|---|
| 834497 | Traffic behaves differently for connected routes and IGP routes in an ADVPN or SD-WAN environment. |
| 836077 | IPv6 SD-WAN health check is not working after a disconnection. |
| 838091 | Static routes from DHCP option 121 are not installed on the FortiGate acting as the DHCP client. |
| 838907 | IPv6 link local address is added into the routing table. |
| 839669 | Static route through an IPsec interface is not removed after the BFD neighbor goes down. |
| 840691 | FortiGate as an NTP server is not using SD-WAN rules. |
| 843345 | OSPF packets are unevenly distributed with the LAG hash algorithm. |
| 847037 | When the policy route has a gateway set, the FortiGate is not following the policy route to forward traffic and sends unreasonable ARP requests. |
| 848270 | Reply traffic from the DNS proxy (DNS database) is choosing the wrong interface. |
| 850862 | GUI does not allow an AS path to be to configured with multiple similar AS numbers. |
| 862165 | FortiGate does not add the route in the routing table when it changes for SD-WAN members. |

## Security Fabric

| Bug ID | Description |
|---|---|
| 809106 | *Security Fabric* widget and *Fabric Connectors* page do not identify FortiGates properly in HA. |
| 814796 | The threat level threshold in the compromised host trigger does not work. |
| 819192 | After adding a Fabric device widget, the device widget does not appear in the dashboard. |
| 822015 | Unable to resolve dynamic address from ACI SDN connector on explicit web proxy. |
| 824433 | After authorizing a downstream FortiGate, an empty name and offline status appear in the device registration wizard. |
| 835765 | Automation stitch trigger is not working when the threshold based email alert is enabled in the configuration. |
| 837347 | Upgrading from 6.4.8 to 7.0.5 causes SDN firewall address configurations to be lost. |
| 839258 | Unable to add another FortiGate to the Security Fabric after updating to the latest patch. |
| 843043 | Only the first ACI SDN connector can be kept after upgrading from 6.4.8 if multiple ACI SDN connectors are configured. |
| 844412 | Security rating failed for custom LLDP profiles. |
| 848822 | *Security Rating* report incorrectly lists the latest AP and switch firmware as unknown. |
| 852340 | Various places in the GUI do not show the secondary HA device. |

| Bug ID | Description |
|---|---|
| 862532 | Unable to load topology pages for a specific Security Fabric topology on the root and downstream FortiGates. |

## SSL VPN

| Bug ID | Description |
|---|---|
| 705880 | Updated empty group with SAML user does not trigger an SSL VPN firewall policy refresh, which causes the SAML user detection to not be successful in later usage. |
| 746230 | SSL VPN web mode cannot display certain websites that are internal bookmarks. |
| 777790 | Unable to select `vip64` in `nat64` firewall policy in the CLI if the `srcintf` is an SSL VPN interface. |
| 783167 | Unable to load GitLab through SSL VPN web portal. |
| 784426 | SSL VPN web mode has problems accessing ComCenter websites. |
| 786056 | VNC using SSL VPN web mode disconnects after 10 minutes. |
| 808107 | FortiGate is not sending Accounting-Request packet that contains the Interim-Update AVP when two-factor authentication is assigned to a user (defined on the FortiGate ) while connecting using SSL VPN. |
| 809717 | EICAR file cannot be blocked through the SSL VPN policy when NTurbo is enabled. |
| 812006 | The PROD-MDN-WS1 SSL VPN portal is not loading properly, and cannot navigate within the page. |
| 818066 | SSL VPN web proxy could not render web application that uses a URL to pass a JSESSIONID |
| 818196 | SSL VPN does not work properly after reconnecting without authentication and a TX drop is found. |
| 819296 | GUI should not use <server_ip> as a sender to send the SSL VPN configuration (it should use value set in `reply-to`). |
| 819754 | Multiple DNS suffixes cannot be set for the SSL VPN portal. |
| 820072 | Unable to open internal website with JavaScript code in SSL VPN web mode. |
| 820536 | SSL VPN web mode bookmark incorrectly applies a URL redirect. |
| 822432 | SSL VPN crashes after copying a string to the remote server using the clipboard in RDP web mode when using RDP security. |
| 822657 | Internal resource pages and menus are not showing correctly in SSL VPN web mode. |
| 823054 | Internal website with JavaScript lacks some menus in SSL VPN web mode. |
| 826083 | Unresponsive portal bookmark in SSL VPN web mode for server that does not support OpenSSL 3.0.2. |
| 829663 | A log in page display error occurs when using an SSL VPN web proxy. |

| Bug ID | Description |
|---|---|
| 829955 | When using SSL VPN to do auto-reconnect without authentication, it always fails the second time it tries to reconnect. |
| 830824 | Veeam Backup Enterprise website has SSL VPN access problem in web mode. |
| 834713 | Getting re-authentication pop-up window for VNC quick connection over SSL VPN web proxy. |
| 837028 | Internal website cannot be displayed correctly in SSL VPN web mode. |
| 839261 | SSL VPN settings are not reflecting any changes when `source-address-negate` is enabled in the CLI. |
| 839743 | Opening an SSL VPN web portal bookmark results in a blank page. |
| 841788 | In policy-based NGFW mode, SSL VPN web mode access does not follow the firewall policy, accept for all destination addresses. |
| 844175 | SSL VPN web mode failed to load some modules for internal website. |
| 847501 | Internal website http://oc***.di***.com dropdown menu on an SSL VPN web mode bookmark in always stays on and does not close. |
| 848067 | RDP over VPN SSL web mode stops work after upgrading. |
| 848312 | Unable to open a PDF in SSL VPN web mode. |
| 848437 | The sslvpn process crashes if a POST request with a body greater than 2 GB is received. |
| 853556 | The http://www.op***.org website does not work in SSL VPN web mode. |
| 856316 | Browser displays an *Error, Feature is not available* message if a file larger than 1 MB is uploaded from FTP or SMB using a web bookmark, even though the file is uploaded successfully. There are no issues with downloading files. |
| 864417 | In the second authentication of RADIUS two-factor authentication, the `acct-update-interval` returned is `0`. SSL VPN uses the second return and not send RADIUS `acct-interim-update` packet. |

# Switch Controller

| Bug ID | Description |
|---|---|
| 818116 | Add link status to managed FortiSwitch switch ports. |
| 836604 | The `40000cr4` port speed is not available under the `switch-controller managed-switch` port speed settings. |
| 840310 | Managed FortiSwitch only shows one port of the FortiLink aggregate interface. |
| 858113 | Unable to view the *Diagnostics and Tools* page for FortiSwitch with limited access permissions using an administrative profile created on the FortiGate. |

# System

| Bug ID | Description |
|---|---|
| 686135 | The dnp process goes to 100% CPU usage as soon as the configuration is downloaded via SCP. Affected platforms: FGR-60F and FGR-60F-3G4G. |
| 724085 | Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected. |
| 748409 | Client traffic from VLAN to VXLAN encapsulation traffic is failing after upgrading. |
| 751715 | Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed. |
| 757482 | When `fastpath` is disabled, counters in the dashboard are showing 0 bytes TX/RX for a VLAN interface configured on an LACP interface. |
| 775793 | Traffic shaping statistics do not work with NP7 offloading. |
| 780315 | Poor CPS performance with VLAN interfaces in firewall only mode (NP7 and NP6 platforms). |
| 782962 | PSU alarm log and SNMP trap are added for FG-10xF and FG-8xF models. |
| 784169 | When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port. |
| 787929 | Deleting a VDOM that contains EMAC interfaces might affect the interface bandwidth widget of the parent VLAN. |
| 798091 | After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation. |
| 798303 | The threshold for conserve mode is lowered. |
| 798992 | Get newcli crash when running the `diagnose hardware test memory` command. |
| 800615 | After a device reboot, the modem interface sometimes does not have a stable route with the local carrier. |
| 801040 | Session anomaly was incorrectly triggered though concurrent sessions on the FortiGate that were below the configured threshold. |
| 805122 | In FIPS-CC mode, if `cfg-save` is set to `revert`, the system will halt a configuration change or certificate purge. |
| 805345 | In some cases, the HA SNMP OID responds very slowly or does work correctly. |
| 809030 | Traffic loss occurs when running SNAT PBA pool in a hyperscale VDOM. The NP7 hardware module PRP got stuck, which caused the NP7 to hang. |
| 810879 | DoS policy ID cannot be moved in GUI and CLI when enabling multiple DoS policies. |
| 813162 | Kernel panic occurs after traffic goes through IPsec VPN tunnel and EMAC VLAN interface. |

| Bug ID | Description |
|---|---|
| 815360 | NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time. |
| 815692 | Slow upload speeds when connected to FIOS connection. Affected platforms: NP6Lite and NP6xLite. |
| 816385 | When creating an inner VLAN CAPWAP interface or sending inner VLAN traffic when the FortiGate is rebooting/upgrading from `capwap-offload disable` status, these actions trigger a freeze. Affected platforms: NP7 models. |
| 818240 | Running `get system performance status` does not update the data. |
| 818452 | The `ifLastChange` SNMP OID only shows zeros. |
| 819460 | There is no `1000auto` option under the ports. Affected platforms: FG-110xE. |
| 819667 | 1G copper SFP port is always up on FG-260xF. |
| 821366 | PPPoE is not working on FG-60E wan2 interface. |
| 822297 | Polling fgfwpolid returns disabled policies. |
| 823589 | When pushing a script from FortiManager to FortiGate, FortiOS will sometimes send the CLI change to FortiManager with the FGFM API. If the tunnel is not up, the session will not exist and it causes a code crash. |
| 824464 | CMDB checksum is not updated when a certificate is renewed over CMP, causing a FortiManager failure to synchronize with the certificate. |
| 824528 | The cid process is consuming high memory, and the FortiGate enters conserve mode. |
| 824543 | The `reply-to` option in the email server settings is no longer visible in a default server configuration on FortiOS 7.2.0. |
| 826440 | Null pointer causing kernel crash on FWF-61F. |
| 827240 | FortiGate in HA may freeze and reboot. Before the reboot, softIRQ may be seen as high. This leads to a kernel panic. |
| 827736 | As the size of the internet service database expands, `ffdb_err_msg_print: ret=-4, Error: kernel error` is observed frequently on 32-bit CPU platforms, such as the FG-100E. |
| 829598 | Constant increase (3%-4%) in memory occurs everyday. |
| 831486 | HQIP memory test failed and triggered a log out with a newcli process crash. |
| 832154 | The cmdbsvr process may crash when there are many addresses and address groups that include each other recursively. |
| 832429 | Random kernel panic may occur due to an incorrect address calculation for the internet service entry's IP range. |
| 832948 | Signature updating from FortiManager does not work after cloud communication is disabled. |
| 832982 | High fcnacd usage occurs and unable to retrieve EMS information from the FortiGate CLI. |
| 834138 | Kernel panic occurs due to VXLAN. |

| Bug ID | Description |
|---|---|
| 834414 | When the uplink modem is restarted, the FortiGate interface configured as PPPoE is unable to obtain an IP address. |
| 834641 | Unable to remove DDNS entry frequently, even if the DDNS setting is disabled. |
| 834762 | Kernel panics occurs on secondary HA node on NP7 models (7.0.6). |
| 835221 | FG-4400F setting speed of `40000full` on QSFP port is not applied at the NIC level. |
| 836049 | Unexpected device reboots with the kernel panic error on NP7 models. |
| 836409 | When deleting a non-existing entry, the error code returned is not appropriate. |
| 837110 | Burst in multicast packets is causing high CPU usage on multiple CPU cores. |
| 837730 | Trusted hosts are not working correctly in FortiOS 7.2.1. |
| 838933 | DoS anomaly has incorrect threshold after loading a modified configuration file. |
| 839190 | Running `get system auto-update versions` causes newcli to crash and the prints quit at the MAC address database. |
| 840175 | Random kernel panic occurs and causes the device to reboot. |
| 841932 | The GUI and API stopped working after loading many interfaces due to httpsd stuck in a D state (kernel I/O socket). |
| 844316 | IPS and application control is causing the FortiGate (VWP) to change either the source MAC address or the destination MAC address based on the flow. |
| 844937 | FG-3700D unexpectedly reboots after the COMLog reported a kernel panic due to an IPv6 failure to set up the master session for the expectation session under some conditions. |
| 845781 | Kernel panic and regular reboots occur on NP7 platforms, which are caused by FortiOS trying to offload a receiving ESP packet from the EMAC VLAN interface and convert to an IPv6 destination address with NAT46 NPU offloaded sessions. |
| 847077 | `Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug. |
| 849186 | Unexpected console error appears: `unregister_netdevice: waiting for pim6reg1 to become free. Usage count = 3`. |
| 850430 | DHCP relay does not work properly with two DHCP relay servers configured. |
| 850797 | Remote access management from a FortiManager login fails if trusted hosts are configured for the administrator account. |
| 852562 | Huge configuration files cause delays during the booting process. |
| 853794 | Issue with the `server_host_key_algorithm` compatibility when using SSH on SolarWinds. |
| 855151 | There may be a race condition between the CMDB initializing and the customer language file loading, which causes the customer language file be removed after upgrading. |
| 856202 | Random reboots and kernel panic on NP7 cluster when the FortiGate sends a TCP RST packet and IP options are missing in the header. |

| Bug ID | Description |
|---|---|
| 859717 | The FortiGate is only offering the `ssh-ed25519` algorithm for an SSH connection. |
| 860052 | The 40G/100G port goes down on FG-260xF when upgrading to 7.2. |
| 862941 | GUI displays a blank page if `vdom-admin` user has partial permissions. |

## Upgrade

| Bug ID | Description |
|---|---|
| 803041 | Link lights on the FG-1100E fail to come up and are inoperative after upgrading. |
| 822844 | Observed `Node exiting due to unhandled rejection` error messages in crash log after upgrading to 7.2.1. |
| 832943 | Upgrading from 7.0.5 (split-VDOM mode) to 7.2.0 converts to multi-VDOM). Certificates are not exported in the backup configuration. |
| 841808 | Traffic counters in `diagnose sys modem history` become empty after upgrading from 6.4. |
| 850691 | The `endpoint-control fctems` entry `0` is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the `endpoint-control fctems` feature was not enabled previously. This leads to a FortiManager installation failure. |

## User & Authentication

| Bug ID | Description |
|---|---|
| 810033 | The samld process is killed if the SP certificate set has an ECC 384-bit public key. |
| 818163 | Remote RADIUS user password change does not work if password encoding is ISO-8859-1 on the FortiGate. |
| 819309 | Unable to create a new guest user if its ID is the ASCII code of a character that is the name of a local user. |
| 820989 | The `srchwvendor`, `devtype`, `srcfamily`, `osname`, and `srchwversion` log fields are not populated properly if the devices are behind a router or proxy. |
| 822684 | When multiple FSSO CA connections are configured at the same time, only the last configured FSSO connection comes up. |
| 822923 | When a device is detected as vulnerable, its source is not set and the inventory query quits. |
| 823227 | FortiGate is adding the same LDAP server in the list of LDAP servers to try twice in fnbamd. |

| Bug ID | Description |
|---|---|
| 824999 | Subject Alternative Name (SAN) is missing from the certificate upon automatic certificate renewal made by the FortiGate. |
| 825505 | Devices are lost in *Users & Devices* widget after a period of time (around two days) in configurations with FortiSwitch, FortiAP, and DHCP. |
| 825759 | The *Device detection* option is missing in the GUI for redundant interfaces (CLI is OK). |
| 827458 | A *User device store query error (error code: -1)* warning appears on the *Asset Identity Center* page. |
| 828212 | RADIUS Access Request message needs to be sent when the client reconnects during firewall authentication session expiration. |
| 829343 | Unknown CA issue can be bypassed when connecting Fortinet hosted servers. |
| 829656 | The device identification scanner crashes due to delayed fragments. |
| 833802 | RADIUS re-authentication is not following RFC 2865 standards. |
| 836082 | LLDP packets are not being received if mgmt is used as an HA management reservation interface. |
| 839801 | FortiToken purge in a VDOM clears all FortiToken statuses in the system. |
| 841566 | The cid process crashes when cloning of 60000 security policies. |
| 842517 | Adding a local user to a group containing many users causes a delay in GUI and CLI due to cmdbsvr (high CPU). |
| 843528 | RADIUS MAC authentication using ClearPass is intermittently using old credentials. |
| 856370 | The EAP proxy worker application crashes frequently. |

## VM

| Bug ID | Description |
|---|---|
| 798717 | Traffic/session logging incorrectly refers to SR-IOV secondary interfaces when the Rx is from fast path. |
| 820457 | Dynamic address objects are removed after Azure API call failed and caused legitimate traffic drop. |
| 825464 | Every time the FortiGate reboots, the certificate setting reverts to `self-sign` under `config system ftm-push`. |
| 848279 | SFTP backup not working with Azure storage account. |
| 859165 | Unable to enable FIPS cipher mode on FG-VM-ARM64-AWS. |
| 859589 | VPNs over Oracle Cloud stop processing traffic. |

## Web Application Firewall

| Bug ID | Description |
|---|---|
| 817673 | Problem accessing some web servers when WAF and AV are enabled in same policy (proxy inspection mode). |
| 838913 | The WAF is indicating malformed request false positives caused by incorrect setups of four known headers: Access-Control-Max-Age, Access-Control-Allow-Headers, Access-Control-Allow-Methods, and Origin. |

## Web Filter

| Bug ID | Description |
|---|---|
| 742483 | System events logs randomly contain a `msg=UrlBwl-black gzopen fail` message. |
| 816781 | FGSP cluster with UTM blocks websites when NTurbo or offloading is enabled. |
| 829628 | Support matching IPv4 mapped IPv6 hostnames in the URL filter. |
| 829704 | Web filter is not logging all URLs properly. |
| 847676 | `Unrated` is displayed, even if the system language is set to Japanese when the policy inspection mode is set to flow. |

## WiFi Controller

| Bug ID | Description |
|---|---|
| 807605 | FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA. |
| 807713 | FortiGate is not sending RADIUS accounting message consistently to RADIUS server for wireless SSO. |
| 809623 | CAPWAP traffic is dropped when `capwap-offload` is enabled. |
| 811953 | Configuration installation from FortiManager breaks the quarantine setting, and the VAP becomes undeletable. |
| 821320 | FG-1800F drops wireless client traffic in L2 tunneled VLAN with `capwap-offload` enabled. |
| 821803 | Wireless multicast traffic causes the cw_acd process to have high CPU usage and triggers a hostapd crash. |
| 824441 | Suggest replacing the *IP Address* column with *MAC Address* in the *Collected Email* widget. |

| Bug ID | Description |
|---|---|
| 827902 | CAPWAP data traffic over redundant IPsec tunnels failing when the primary IPsec tunnel is down (failover to backup tunnel). |
| 828901 | Connectivity loss occurs due to switch and FortiAPs (hostapd crash). |
| 831736 | Application hostapd crash found on FG-101F. |
| 831932 | The cw_acd process crashes several times after the system enters conserve mode. |
| 834644 | A hostapd process crash is shown in device crash logs. |
| 837130 | Wireless client shows portal related webpage while doing MAC authentication with MAB mode. |
| 840717 | CAPWAP daemon(cw_acd) experiences a signal 11 crash when reconnecting a FortiAP to the FortiGate, and the FortiGate does not populate SA scan data on `radio0` and `radio1` of 231G when starting the SA from the FGT FortiGate GUI. |
| 844172 | The cw_acd process is deleting dynamic IPsec tunnels on the secondary device, which causes the FortiAPs to disconnect on the primary device. |
| 846730 | *Dynamic VLAN assignment* is disabled in the GUI when editing an SSID with `radius mac-auth` and `dynamic-vlan` enabled. |
| 856830 | HA FortiGate encounters multiple hostapd crashes. |
| 857140 | Hostapd segmentation fault signal 11 occurs upon RF chamber setup. |
| 857975 | The cw_acd process appears to be stuck, and is sending several access requesst for MAC authentication. |
| 858653 | Invalid wireless MAC OUI detected for a valid client on the network. |
| 861552 | Wireless client gets disconnect from WiFi if it is connected to a WPA2 SSID more than 12 hours. |

## ZTNA

| Bug ID | Description |
|---|---|
| 792829 | WAD re-challenges user authentication upon HA failover. |
| 832508 | The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.2.1 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`.<br>After upgrading from 7.2.0 to 7.2.1, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled. |
| 845321 | An offline FortiClient should be immediately rejected by ZTNA. |
| 848222 | ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. |

| Bug ID | Description |
|---|---|
| | An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found. |
| 859421 | ZTNA server (access proxy VIP) is causing all interfaces that receive ARP request to reply with their MAC address. |
| 875589 | WAD crash observed when a client EMS tag changes. |

# Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

| Bug ID | CVE references |
|---|---|
| 844920 | FortiOS 7.2.4 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-41328 |
| 853448 | FortiOS 7.2.4 is no longer vulnerable to the following CVE Reference:<br>• CVE-2022-42475 |
| 855446 | FortiOS 7.2.4 is no longer vulnerable to the following CVE References:<br>• CVE-2022-3602<br>• CVE-2022-3786 |

# Known issues

The following issues have been identified in version 7.2.4. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

## Explicit Proxy

| Bug ID | Description |
|---|---|
| 875736 | The `proxy-re-authentication-mode` option has been removed in 7.2.4 and is replaced with `proxy-keep-alive-mode re-authentication`. The new `proxy-re-authentication-time` timer is associated with this re-authentication mode. There are two unresolved issues:<br>• After upgrading, the previously configured `proxy-auth-timeout` value for the absolute re-authentication mode is not preserved in the new `proxy-re-authentication-time`.<br>• The new `proxy-re-authentication-time` is currently configured in seconds, but it should be configured in minutes to be consistent with other related authentication timers (such as `proxy-auth-timeout`). |
| 877337 | HTTPS requests over IPv6 are not matched sometimes to the proxy policy when the IPv6 Internet Service Database is applied in the proxy policy. |

## Firewall

| Bug ID | Description |
|---|---|
| 770541 | There is a delay opening firewall, DoS, and traffic shaping policies in the GUI. |
| 860480 | FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later. |
| 861990 | Increased CPU usage in softIRQ after upgrading from 7.0.5 to 7.0.6. |

## GUI

| Bug ID | Description |
|---|---|
| 677806 | On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status. |

| Bug ID | Description |
|---|---|
| 699508 | When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in. |
| 853352 | On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries. |

## Hyperscale

| Bug ID | Description |
|---|---|
| 802182 | A `cmdb_txn_cache_data(query=log.npu-server,leve=1) failed` error is seen after editing an interface's VLAN ID. |
| 807523 | On NP7 platforms the `config system npu` option for `nat46-force-ipv4-packet-forwarding` is missing. |
| 829549 | DSE entry is being created for ALG sessions, and EIF sessions pass through. |
| 841712 | The `nat64-force-ipv4-packet-forwarding` command is missing under `config system npu` |
| 843197 | Output of `diagnose sys npu-session list/list-full` does not mention policy route information. |
| 846520 | NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover. |
| 872146 | The `diagnose sys npu-session list` command shows an incorrect policy ID when traffic is using an intra-zone policy. |

## Intrusion Prevention

| Bug ID | Description |
|---|---|
| 813727 | Custom signatures are not shown in the list when filters (server, client, or critical severity) are applied in an IPS sensor. |

## IPsec VPN

| Bug ID | Description |
|---|---|
| 699973 | IPsec aggregate shows down status on *Interfaces*, *Firewall Policy*, and *Static Routes* configuration pages. |

## Proxy

| Bug ID | Description |
|---|---|
| 827807 | WAD crash at signal 11 is observed after configuring 250 CGN VDOMs (`full-offload` is enabled on the VDOM). |
| 837724 | WAD crash occurs. |

## Security Fabric

| Bug ID | Description |
|---|---|
| 814674 | *Failed to retrieve upgrade progress* message appears when upgrading a FortiAP or FortiSwitch that is connected to a downstream FortiGate. |
| 825291 | FortiAnalyzer connection security rating fails for FortiAnalyzer Cloud. |

## SSL VPN

| Bug ID | Description |
|---|---|
| 719740 | The *No SSL-VPN policies exist* warning should not be shown in the GUI when a zone that has ssl.root as a member is set in an SSL VPN policy. |
| 795381 | FortiClient Windows cannot be launched with SSL VPN web portal. |

## Switch Controller

| Bug ID | Description |
|---|---|
| 813216 | FortiLink goes down when CAPWAP offloading is enabled or disabled. |

## System

| Bug ID | Description |
|---|---|
| 725048 | Performance improvements for `/api/v2/monitor/system/available-interfaces` (phase 2). |
| 776646 | Configuring a delegated interface to obtain the IPv6 prefix from an upstream DHCPv6 server in the GUI fails with a CLI internal error. |
| 818795 | Kernel panic observed on FG-3700D. |

## User & Authentication

| Bug ID | Description |
|---|---|
| 813969 | SAML SSO login for VDOM administrator still works when logging in to the FortiGate and the connecting interface does not belong to that VDOM. |

## Web Filter

| Bug ID | Description |
|---|---|
| 766126 | Block replacement page is not pushed automatically to replace the video content when using a video filter. |

## WiFi Controller

| Bug ID | Description |
|---|---|
| 789072 | Kernel panic on FWF-61F due to `ol_target_failure, Target Register Dump Location 0x00401AE0`. |
| 790973 | FG-2500E drops CAPWAP traffic when a client is connected with a VLAN SSID and NP6 offloading is enabled. |
| 814541 | On a FortiGate managing 1200 FortiAPs and over 7000 clients, the *Dashboard* > *Status* page and *FortiAP Status* widget are slow to load. |
| 868022 | Wi-Fi clients on a RADIUS MAC MPSK SSID get prematurely de-authenticated by the secondary FortiGate in the HA cluster. |

| Bug ID | Description |
|---|---|
| 869106 | The layer 3 roaming feature may not work when the wireless controller is running multiple cw_acd processes (when the value of `acd-process-count` is not zero). |
| 869978 | CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled on FG-200F. |

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com